Transportation Security Administration

**OFFICE OF INFORMATION TECHNOLOGY**

**TSA MANAGEMENT DIRECTIVE No. 1400.3**
**INFORMATION TECHNOLOGY SECURITY**

***To enhance mission performance, TSA is committed to promoting a culture founded on its values of Integrity, Innovation and Team Spirit.***

**REVISION:** This revised directive supersedes TSA MD 1400.3, *Information Technology Security* dated October 5, 2010.

**SUMMARY OF CHANGES:** Section 1, Purpose, revised; Section 2, Scope, updated; Section 4, Definitions, revised; Section 5, Responsibilities, revised; Section 6, Policy, updated; and Section 7, Procedures, revised.

1. **PURPOSE:** This directive provides TSA policy and procedures for the secure use, development, and maintenance of TSA information systems including prototypes and telecommunications.

2. **SCOPE:** This directive and the *TSA Information Assurance Handbook* apply to all TSA employees and contractors, as well as TSA-owned or TSA-controlled information systems that collect, generates, process, store, display, transmit, or receive TSA data. This includes prototypes, telecommunications systems, and all systems in all phases of the System Engineering Life Cycle (SELC).

3. **AUTHORITIES:**

   A. 14 Code of Federal Regulations (CFR), Part 191, *Protection of Sensitive Security Information*

   B. 44 United States Code (USC) Chapter 33, *Disposal of Records*

   C. *Computer Fraud and Abuse Act of 1986*

   D. *Computer Security Act of 1987*

   E. DHS 140-01, *Information Technology Systems Security*

   F. DHS *Sensitive Systems Policy Directive* 4300A

   G. DHS *National Security Systems Policy Directive* 4300B

   H. *E-Government Act of 2002*, Public Law 107-347

   I. E.O. 13526, *Classified National Security Information*

   J. *Federal Information Security Management Act (FISMA) of 2002*

   K. Homeland Security Presidential Directive (HSPD) 7, *Critical Infrastructure Identification, Prioritization, and Protection* (Supersedes Presidential Decision Directive-63)

   L. HSPD 12, *Policy for a Common Identification Standard for Federal Employees and Contractors*

M. National Institute of Standards and Technology (NIST) Special Publication 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems*

N. NIST Special Publication 800-55, *Security Metrics Guide for Information Security*

O. *Privacy Act of 1974*, as amended

P. Public Law (PL) 99-508, *Electronic Communications Privacy Act of 1986*

Q. Revision of Office of Management and Budget (OMB) Circular A-130, Appendix III, *Security of Federal Automated Information Resources*

R. Title 36, CFR, Chapter XII, Subchapter B, *Records Management*

4. **DEFINITIONS:** See the *TSA Information Assurance Handbook* for additional definitions.

A. Authorizing Official (AO): TSA official with the authority to formally assume accountability for operating an information system at an acceptable level of risk to the agency and is empowered to grant and oversee approval for a system to operate.

B. Chief Information Officer (CIO): TSA official with oversight authority for information systems and the effectiveness and completeness of each system's Information Security including FISMA compliance within the Agency.

C. Chief Information Security Officer (CISO): TSA official with assigned authority and oversight for implementing and organizing information security program under the direction of the CIO. This position may also be known as the Senior Information Security Officer.

D. Information Owner: TSA official with statutory or operational authority for specified information and oversight on establishing controls for its generation, collection, processing, dissemination, and disposal.

**NOTE:** With some systems the Information Owner may also be the Program Manager, Business Owner or System Owner.

E. Information System Security Officer (ISSO): The security official, either government or contractor, responsible for the security posture of an assigned set of information systems.

F. Information System: A discrete set of information resources, either in stand-alone or networked configurations, which is organized for the collection, processing, maintenance, transmission, and dissemination of information in accordance with defined procedures, whether automated or manual.

G. Security Authorization Package: The package that is transmitted from the System Owner to the AO seeking an official management decision to authorize operation of a an information system for all offices in a specified environment at an acceptable level of risk, based on the implementation of an approved set of technical, managerial, and operational safeguards.

H. Security Authorization Process: The combination of documentation, test and evaluation activities required to ensure that adequate information security controls are in place to reduce the information security risks of operating a system to an acceptable level and acknowledgement that the level of residual risk is acceptable to management.

I. Security Control Assessor (SCA): The individual, group, or organization with the authority and oversight for conducting the security control assessment.

J. System Engineering Life Cycle (SELC): The set of processes used by a systems analyst to develop an information system, including requirements, validation, training, and user ownership.

K. System Owner (SO): The Government official responsible for implementing and maintaining the security posture of an assigned set of information systems.

5. **RESPONSIBILITIES:** See the *TSA Information Assurance Handbook* for additional responsibilities.

A. The CIO is responsible for:

(1) Developing and maintaining the TSA Information Security Program;

(2) Appointing AOs for every TSA information system or serving as the AO for information systems where no AO has otherwise been appointed, or where a vacancy exists;

(3) Appointing a Chief Information Security Officer (CISO); and

(4) Ensuring that information security requirements are addressed early in the acquisition and contracting process.

B. The AO is responsible for:

(1) Ensuring the operation of an information system is at an acceptable level of risk to an agency;

(2) Granting or withholding authorization of the security controls prescribed for a system; and

(3) Signing an authorization memorandum that documents the authorization decision determined by the adequacy of system safeguards.

C. The CISO is responsible for:

(1) Implementing and managing the TSA-wide Information Security program;

(2) Issuing TSA-wide information security policy, guidance, and architectural requirements for all TSA information systems and networks;

(3) Serving as the principal department liaison with organizations outside TSA in matters relating to information security; and

(4) Arbitrating a conflicting information security policy or guidance.

D. The SCA is responsible for:

(1) Ensuring that risk analysis is performed to identify security risks;

(2) Determining risk magnitude; and

(3) Identifying what areas need additional safeguards.

E. The SO is responsible for:

(1) Procuring, developing, integrating, modifying, operating, maintaining, retiring and disposing of an information system;

(2) Ensuring that information security requirements are included in the acquisition process and considered throughout the lifecycle of the IT system; and

(3) Ensuring that required security authorization activities are completed and the results are documented and updated annually.

F. The ISSO is responsible for performing all specific tasking as defined in the DHS *Information System Security Officer (ISSO) Guide* and the specific TSA ISSO appointment letter.

G. TSA offices that acquire, develop, own, operate, or replace information system components, and lines of business are responsible for:

(1) Participating in the formulation and approval of TSA IT security policies, requirements, procedures, and IT security risk mitigation strategies;

(2) Ensuring FISMA requirement security initiatives are cost effective and technically efficient; and

(3) Ensuring information security requirements are properly budgeted as part of the overall acquisitions process. These requirements shall consider costs pertaining to the procurement, operations, maintenance, licensing, retirement and disposition of IT systems and/or products in accordance with applicable TSA and DHS policies.

H. All TSA employees, contractors, detailees, and others working on behalf of DHS, and users of TSA information systems are responsible for supporting and complying with IT security program requirements stated herein.

I. The Contracting Officer (CO) is responsible for ensuring the use of information security verbiage is considered and incorporated into contracts, as required.

6. **POLICY:**

   A. TSA employees, contractors and information systems covered under the scope of this directive shall uphold the security requirements in accordance with the accompanying *TSA Information Assurance Handbook* and all applicable DHS policies to ensure that all TSA information systems, assets, and information are secured.

   B. TSA employees, contractor, and information systems covered under the scope of this directive shall support the secure development, use, maintenance, retirement, and disposal of TSA information systems, information and networks, including prototypes and telecommunications systems.

   C. The DHS *Sensitive Systems Policy Directive* 4300A and its supporting handbook shall take precedence in instances where there is conflict with TSA MD 1400.3 and its supporting handbook, unless otherwise indicated in TSA policy.

   D. Each TSA office directly reporting to the Administrator shall obtain formal security authorization for its information systems from the appropriate AO in accordance with the *TSA Information Assurance Handbook*.

   E. All TSA employees and contractors shall receive and complete adequate annual information security awareness and privileged user training, (if applicable).

   F. All policy and supporting documentation established as a result of this directive shall be maintained on the TSA OIT Policy website.

7. **PROCEDURES:** Refer to the TSA OIT Policy website to access establishment and maintenance procedures as outlined by the *TSA Information Assurance Handbook,* technical standards, the Online Learning Center (OLC), and additional publications that provide the foundation to ensure confidentiality, integrity, availability, reliability, and non-repudiation within the TSA IT enterprise, IT infrastructure and operations.

8. **APPROVAL AND EFFECTIVE DATE:** This policy is approved and effective the date of signature unless otherwise specified.

**APPROVAL**

***Signed*** **April 8, 2014**

_____ _____
Stephen Rice Date
Assistant Administrator
Chief Information Officer
Office of Information Technology

**EFFECTIVE**

_____
Date

Distribution: All TSA employees and contract personnel
Point of Contact: OIT, Information Assurance and Cyber Security Division (IAD), TSAIADPolicy@tsa.dhs.gov, 571-227-2490